

## PATENT ABSTRACTS OF JAPAN

(11)Publication number : 10-222063

(43)Date of publication of application : 21.08.1998

(51)Int.Cl.

G09C 1/00

G06F 15/00

H04L 9/32

(21)Application number : 09-035474

(71)Applicant : VICTOR CO OF JAPAN LTD

(22)Date of filing : 04.02.1997

(72)Inventor : SHISHIDO ICHIRO

**(54) DIGITAL INFORMATION MANAGEMENT SYSTEM, TERMINAL DEVICE, INFORMATION MANAGEMENT CENTER, AND METHOD OF CONTROLLING DIGITAL INFORMATION**

(57)Abstract:

**PROBLEM TO BE SOLVED:** To make it possible to prevent illegal copy without losing convenience for proper users.

**SOLUTION:** When digital information is used, a registration number and a registration number authentication corresponding to the digital information used from a terminal equipment 2 are transmitted to an information management center 1. The information management center 1 examines a validity of the received registration number and also checks the conditions for the use of the corresponding digital information, and transmits data indicating a permission for the use if the number has a validity, and transmits data for inhibiting the use to terminal device 2, if the number is not duly permitted for the use. The terminal device 2 is arranged so that the digital information is usable thereon only when it receives a permission for the use.

**LEGAL STATUS**

[Date of request for examination] 17.03.2000

[Date of sending the examiner's decision of rejection] 17.10.2003

[Kind of final disposal of application other than the examiner's decision of rejection or application converted registration]

[Date of final disposal for application]

[Patent number]

[Date of registration]

[Number of appeal against examiner's decision of rejection]

[Date of requesting appeal against examiner's decision of rejection]

[Date of extinction of right]

Copyright (C); 1998,2003 Japan Patent Office

(19)日本国特許庁 (J P)

(12) 公 開 特 許 公 報 (A)

(11)特許出願公開番号

特開平10-222063

(43)公開日 平成10年(1998) 8月21日

(51)Int.Cl.<sup>6</sup>  
G 0 9 C 1/00  
G 0 6 F 15/00  
H 0 4 L 9/32

識別記号  
6 4 0  
3 3 0

F I  
G 0 9 C 1/00  
G 0 6 F 15/00  
H 0 4 L 9/00  
6 4 0 B  
3 3 0 Z  
6 7 5 D  
6 7 6 B

審査請求 未請求 請求項の数7 F D (全 10 頁)

(21)出願番号 特願平9-35474

(22)出願日 平成9年(1997) 2月4日

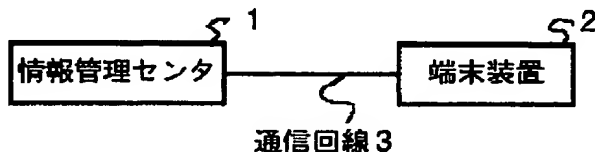
(71)出願人 000004329  
日本ビクター株式会社  
神奈川県横浜市神奈川区守屋町3丁目12番  
地  
(72)発明者 穴戸 一郎  
神奈川県横浜市神奈川区守屋町3丁目12番  
地 日本ビクター株式会社内

(54)【発明の名称】 デジタル情報管理システム、端末装置、情報管理センタ及びデジタル情報管理方法

(57)【要約】

【課題】 正当な利用者の利便性を損なうことなく、不正コピーを防止することができなかった。

【解決手段】 デジタル情報を使用する際に、端末装置2から使用するデジタル情報に対応する登録番号と登録番号認証子とを情報管理センタ1に送信する。情報管理センタ1では受信した登録番号の正当性を検査すると共に該当するデジタル情報の使用条件を確認し、正当に使用可能な状態であれば使用許可を示すデータを端末装置2に送信し、正当に使用することができない状態であれば使用禁止を示すデータを端末装置2に送信する。端末装置2では使用許可を示すデータを受信した時のみデジタル情報を使用できるようにする。



## 【特許請求の範囲】

【請求項 1】 端末装置と情報管理センタとが通信回線を介して接続され、前記端末装置に記憶されているデジタル情報の管理を行うデジタル情報管理システムであって、

前記端末装置は、前記情報管理センタとの通信を行う第 1 の通信手段と、前記デジタル情報を識別する登録番号と登録番号認証子と前記デジタル情報本体とを格納するデジタル情報格納手段と、前記デジタル情報の利用手順を制御する第 1 の制御手段とで構成され、

前記情報管理センタは、前記端末装置との通信を行う第 2 の通信手段と、前記登録番号とその使用条件を記憶格納する使用条件格納手段と、前記認証子を使って前記登録番号を認証する認証処理手段と、前記情報管理センタ全体を制御する第 2 の制御手段とで構成されることを特徴とするデジタル情報管理システム。

【請求項 2】 情報管理センタとの通信を行う通信手段と、デジタル情報を識別する登録番号と登録番号認証子とデジタル情報本体とを格納するデジタル情報格納手段と、前記デジタル情報の利用手順を制御する制御手段とで構成されたことを特徴とする端末装置。

【請求項 3】 前記登録番号あるいは前記登録番号の認証子の特定の部分のビット列と前記デジタル情報本体の特定の部分のビット列が一致するように前記登録番号が設定されており、前記デジタル情報格納手段において前記一致するビット列を重ね合わせて配置することを特徴とする請求項 2 記載の端末装置。

【請求項 4】 端末装置との通信を行う通信手段と、登録番号とその使用条件を記憶格納する使用条件格納手段と、前記認証子を使って前記登録番号を認証する認証処理手段と、前記各手段を制御する制御手段とで構成されたことを特徴とする情報管理センタ。

【請求項 5】 前記登録番号あるいは前記登録番号の認証子の特定の部分のビット列と前記デジタル情報本体の特定の部分のビット列が一致するように前記登録番号を設定することを特徴とする請求項 4 記載の情報管理センタ。

【請求項 6】 端末装置に記憶されているデジタル情報の管理を行うデジタル情報管理方法であって、

前記端末装置から前記デジタル情報を識別する登録番号と登録番号認証子とを通信回線を介して接続されている情報管理センタに送信する第 1 の手順と、

前記情報管理センタにて受信した前記登録番号の正当性を前記登録番号認証子と暗号鍵を用いて確認する第 2 の手順と、

前記情報管理センタにて受信した前記登録番号に該当する前記デジタル情報が前記使用条件に合致しているかを確認する第 3 の手順と、

前記情報管理センタにて前記使用条件に合致していれば、使用許可を示すデータを前記端末装置に送信し、前

記使用条件に合致していなければ、使用禁止を示すデータを前記端末装置に送信する第 4 の手順と、

前記端末装置にて使用許可を示すデータを受信したときのみ前記デジタル情報を使用できるようにする第 5 の手順とからなることを特徴とするデジタル情報管理方法。

【請求項 7】 前記登録番号認証子として、前記登録番号あるいは前記登録番号を一方向性ハッシュ関数に代入した値を前記情報管理センタの暗号鍵で暗号化した値を用いたことを特徴とする請求項 6 記載のデジタル情報管理方法。

## 【発明の詳細な説明】

## 【0001】

【発明の属する技術分野】 本発明は、端末装置内に蓄積されたデジタル情報の不正利用を防止するデジタル情報管理システム及びにデジタル情報管理方法に係り、特に規定回数や規定期間を越えた場合などを含む不正利用者に対してデジタル情報を利用できないようにするデジタル情報管理システム及びにデジタル情報管理方法に関するものである。

## 【0002】

【従来の技術】 近年、テキスト、音声、静止画、動画等をデジタル化して、コンピュータ上で利用することが急激に増えている。しかしデジタルデータには、コンピュータ上で元データと全く同じものを容易にコピー／作成できるという性質があるので、不正コピーにより著作権者やデータ販売者の権利が侵害されるといった問題が生じている。

【0003】 また最近では、単に不正コピーを防止するだけでなく、データの有用性を理解してもらうために使用回数や使用期間を限定してデータを利用させたり、デジタル動画等を再生する回数に応じて料金を徴収したりしたいというニーズも高まっている。これらの問題解決やニーズを実現する方法としては、例えば特開平 3-2882 27 号が開示されている。これはソフトウェアの使用回数を制限する方法であり、簡単に説明すると、まず、ソフトウェアの提供者が通信手段を介して使用制限回数と使用回数の初期値を利用者のコンピュータ（端末装置）に送出し、それらを利用者のコンピュータ内の記録媒体に記録しておく。そして、ソフトウェア実行時に使用回数を更新すると共に使用制限回数と比較して、使用回数が使用制限回数を越えた場合にソフトウェアの実行を中止するという方法である。

【0004】 しかしこの方法では、利用者のコンピュータ内で使用回数と使用制限回数を記録管理しているので、専用のコンピュータならともかく、一般に仕様が公開されているハードウェアやオペレーティングシステムを使用した、いわゆる一般的なコンピュータ（パーソナルコンピュータ）では、技術レベルの高い利用者が使用回数や使用制限回数を書き換える可能性がある。また、ソフトウェア提供者に対して利用するコンピュータの電

話番号やアドレスを教える必要があるので、手続きの煩雑さやプライバシー保護の点で問題があった。

【0005】また、別の方法が特開平7-131452号に開示されている。これは、端末装置から通信回線を介して情報センタに蓄積されているデジタル情報をダウンロードする際に、その端末装置でのみデジタル情報が利用出来るようにデジタル情報を暗号化すると共に、そのデジタル情報の利用条件をダウンロードし、端末装置内の機密処理部に格納する。そして、情報を利用する際に機密処理部に格納されている決められた使用条件に合うかどうかチェックし、この条件に合わない場合は利用を禁止するという方法である。

【0006】

【発明が解決しようとする課題】この後者の方法では、端末装置内で暗号の共通鍵、使用条件、使用履歴等を格納するための機密処理部が利用者から完全に隠蔽されることが必要となるが、より多くの利用者を獲得する為には、端末装置は一般的な構成のコンピュータ（パーソナルコンピュータ）であることが望ましい。しかし、利用者が不正な方法でも読み書きすることができない耐タンパー性を持つ特殊な装置を付加することなく、ごく一般的な構成のコンピュータでこのような機密処理部を実現することは非常に困難であった。また、特殊な装置を使用すると、端末装置のコストが高くなったり、利用者数が限定されてしまい、実用上問題があった。

【0007】さらに、上記2つの方法では、購入したソフトウェアやデジタル情報を利用出来る端末装置がダウンロードした端末装置1台だけに限定されてしまうので、例えば、正当にデジタル情報を購入した利用者が自宅と職場の両方でそのデジタル情報を利用したいとしても、端末装置を持ち運んで移動させなければそのように利用することは不可能であり、正当な利用者の利便性を損なう恐れがあった。また別の方法として、デジタル情報を利用する際に、その都度サーバからダウンロードを行い、端末装置内にデジタル情報を蓄積させないことによって不正コピーを防止する方法も考えられるが、通信コストが高くなり、ダウンロードにも時間がかかるといった問題があった。

【0008】そこで本発明は、正当な利用者の利便性を損なうことなく、不正コピーを防止し、また、使用回数や使用期間を限定してデータを利用させたり、デジタル動画等を再生する回数に応じて料金を徴収したりすることのできるデジタル情報管理システムを提供することを目的とする。

【0009】

【課題を解決するための手段】上記目的を達成するための手段として、以下に示すデジタル情報管理システム、端末装置、情報管理センタ及びデジタル情報管理方法を提供しようとするものである。

【0010】1. 端末装置と情報管理センタとが通信回

線を介して接続され、前記端末装置に記憶されているデジタル情報の管理を行うデジタル情報管理システムであって、前記端末装置は、前記情報管理センタとの通信を行う第1の通信手段と、前記デジタル情報を識別する登録番号と登録番号認証子と前記デジタル情報本体とを格納するデジタル情報格納手段と、前記デジタル情報の利用手順を制御する第1の制御手段とで構成され、前記情報管理センタは、前記端末装置との通信を行う第2の通信手段と、前記登録番号とその使用条件を記憶格納する使用条件格納手段と、前記認証子を使って前記登録番号を認証する認証処理手段と、前記情報管理センタ全体を制御する第2の制御手段とで構成されることを特徴とするデジタル情報管理システム。

【0011】2. 情報管理センタとの通信を行う通信手段と、デジタル情報を識別する登録番号と登録番号認証子とデジタル情報本体とを格納するデジタル情報格納手段と、前記デジタル情報の利用手順を制御する制御手段とで構成されたことを特徴とする端末装置。

【0012】3. 前記登録番号あるいは前記登録番号の認証子の特定の部分のビット列と前記デジタル情報本体の特定の部分のビット列が一致するように前記登録番号が設定されており、前記デジタル情報格納手段において前記一致するビット列を重ね合わせて配置することを特徴とする上記2. 記載の端末装置。

【0013】4. 端末装置との通信を行う通信手段と、登録番号とその使用条件を記憶格納する使用条件格納手段と、前記認証子を使って前記登録番号を認証する認証処理手段と、前記各手段を制御する制御手段とで構成されたことを特徴とする情報管理センタ。

【0014】5. 前記登録番号あるいは前記登録番号の認証子の特定の部分のビット列と前記デジタル情報本体の特定の部分のビット列が一致するように前記登録番号を設定することを特徴とする上記4. 記載の情報管理センタ。

【0015】6. 端末装置に記憶されているデジタル情報の管理を行うデジタル情報管理方法であって、前記端末装置から前記デジタル情報を識別する登録番号と登録番号認証子とを通信回線を介して接続されている情報管理センタに送信する第1の手順と、前記情報管理センタにて受信した前記登録番号の正当性を前記登録番号認証子と暗号鍵を用いて確認する第2の手順と、前記情報管理センタにて受信した前記登録番号に該当する前記デジタル情報が前記使用条件に合致しているかを確認する第3の手順と、前記情報管理センタにて前記使用条件に合致していれば、使用許可を示すデータを前記端末装置に送信し、前記使用条件に合致していなければ、使用禁止を示すデータを前記端末装置に送信する第4の手順と、前記端末装置にて使用許可を示すデータを受信したときのみ前記デジタル情報を使用できるようにする第5の手順とからなることを特徴とするデジタル情報管理方法。

【0016】7. 前記登録番号認証子として、前記登録番号あるいは前記登録番号を一方向性ハッシュ関数に代入した値を前記情報管理センタの暗号鍵で暗号化した値を用いたことを特徴とする上記6記載のデジタル情報管理方法。

【0017】

【発明の実施の形態】本発明のデジタル情報管理システムは、図1に示すように端末装置2と情報管理センタ1とが通信回線3を介して接続されているシステムであり、情報管理センタ1においてデジタル情報の使用条件及び使用状況を記録管理することが本発明の特徴である。そして、端末装置2は、図2に示すように、情報管理センタ1との通信を行う通信手段（第1の通信手段）4と、デジタル情報を一意に識別可能な登録番号と登録番号の認証子とデジタル情報本体とを格納するデジタル情報格納手段6と、デジタル情報の利用手順を制御する制御手段（第1の制御手段）5と、入力手段8及び出力手段9を有している。

【0018】また、情報管理センタ1は、図3に示すように、端末装置2との通信を行う通信手段（第2の通信手段）101と、登録番号とその使用条件を記憶格納する使用条件格納手段103と、登録番号の認証をおこなう認証処理手段104と、制御手段（第2の制御手段）102とを有している。このような構成のデジタル情報管理システムにおいて、実際にデジタル情報を管理するデジタル情報管理方法について説明する。

【0019】まず、情報販売者は、またはデジタル情報を販売する際に、登録番号と登録番号の認証子をデジタル情報本体に付加すると共に、登録番号とその使用条件を情報管理センタ1の使用条件格納手段103に登録する。ここで、登録番号と登録番号の認証子をデジタル情報本体に付加する方法としては、例えば、デジタル情報があらかじめインストールされていたり、CD-ROMなどの可搬型の記録媒体により供給されていて、デジタル情報が既に端末装置2のデジタル情報格納手段6に格納されている場合には、利用者として登録する際に登録番号と登録番号の認証子を端末装置2に対して通信回線3を介して供給し、デジタル情報を通信回線3を介してダウンロードする場合は、デジタル情報と共に供給すれば良い。

【0020】そして、登録後、利用者が端末装置2でデジタル情報を使用するために、端末装置2の制御手段5に使用する旨の指示を与えると、端末装置2と情報管理センタ1との間で以下の処理が行われた後、デジタル情報が利用可能となる。まず端末装置2は、登録番号と登録番号の認証子を情報管理センタ1に送信する。情報管理センタ1では受信した登録番号に該当するデジタル情報の使用条件を確認し、正当に使用可能な状態であるかを確認する。正当な使用であれば使用許可を示すデータを端末装置2に送信する。もし、正当な使用でなけれ

ば使用禁止を示すデータを端末装置2に送信する。端末装置2では情報管理センタ1から受信したデータが使用許可を示す時のみデジタル情報を使用できるように制御する。

【0021】このような方法を用いることにより、利用者が不正に使用条件を変えることが困難になるので、デジタル情報の使用回数や使用期限を正確に管理することができる。また、本発明における端末装置2は、複雑な処理が必要となる暗号処理部が不要である。また機密保持が必要な共通鍵や秘密鍵を格納していない。さらに利用者から隠蔽する必要のある使用条件や使用履歴を格納していないので、従来例のような機密処理部を必要としない。従って、特殊な装置を付加しない一般的な構成のコンピュータを端末装置2として使った場合でも、デジタル情報の使用回数や使用期限を正確に管理することが可能になる。

【0022】

【実施例】本発明デジタル情報管理システムの一実施例を図面と共に説明する。図1は本実施例の全体の構成を示す図である。同図において、デジタル情報を利用する端末装置2とデジタル情報の使用条件を管理する情報管理センタ1とが、電話回線、専用線、LAN等の通信回線3によって接続されている。そして、この端末装置2の構成例を図2に示す。なお、パーソナルコンピュータで構成した場合には、同図中、点線で示した部分がパソコン本体となり、それに、キーボードやマウスなどの入力手段8及びディスプレイなどの出力手段9が接続されている。点線で囲まれたパソコン本体には、情報管理センタ1との通信を行う通信手段4と、デジタル情報を一意に識別可能な登録番号と登録番号の認証子とデジタル情報本体とを格納するデジタル情報格納手段6と、デジタル情報の利用手順を制御する制御手段5とを有している。

【0023】この通信手段4は、通信回線3の種類に応じてモデムやLANコントローラ等で構成されており、制御手段5の指示により情報管理センタ1との通信を行うものである。デジタル情報格納手段6は、ハードディスク、フロッピーディスク、MOディスク、あるいはその他の不揮発性メモリ等で構成されている。そして、1つのデジタル情報につき、デジタル情報を識別するための登録番号と登録番号の認証子とデジタル情報本体とが格納される。

【0024】制御手段5は、CPU、RAM、ROM等で構成されており、デジタル情報を利用者が利用する際に、決められた手順に従って端末装置2の各部を制御するものである。入力手段8は、キーボード、マウス、操作ボタン、リモコン等で構成されており、利用者が利用するデジタル情報や利用方法を選択した結果の指示を制御手段5に与える為に使用するものである。情報出力手段9は、ディスプレイ、スピーカ、プリンタ等の出力装置で

あり、デジタル情報の種類に応じて、例えば静止画や動画ならばディスプレイ、音声ならばスピーカといったように適切な出力装置が選択される。

【0025】そして、図3に情報管理センタ1の構成を示す。この情報管理センタ1は、端末装置2との通信を行う通信手段101と、使用条件を記憶格納する使用条件格納手段103と、登録番号の認証をおこなう認証処理手段104と、制御手段102とで構成されている。

【0026】使用条件格納手段103には、図4に示す形式の使用条件テーブルが格納されている。図4に示す 10 テーブルにおいて、登録番号は情報管理センタ1で管理するデジタル情報を一意に識別する番号である。この登録番号は端末装置2のデジタル情報格納手段6に格納されている登録番号と同じものである。なお後述するように、登録番号の一部のビット列がデジタル情報本体の一部のビット列と一致するように登録番号を割り当てても良い。また、期間制限フラグは使用期間の制限を行うかどうかを示すフラグであり、使用期間の制限を行う場合は「1」に、行わない場合は「0」に設定されている。回数制限フラグは使用回数の制限を行うかどうかを示す 20 フラグであり、使用回数の制限を行う場合は「1」に、行わない場合は「0」に設定されている。許可開始日時は期間制限フラグが「1」の場合に有効であり、使用許可を開始する年、月日、時刻を示している。許可終了日時は期間制限フラグが「1」の場合に有効であり、使用許可を終了する年、月日、時刻を示している。使用可能回数は回数制限フラグが「1」の場合に有効であり、今後使用可能な回数を示している。したがって、回数制限フラグが「1」であって、このフィールドが「0」になると使用出来なくなる。そして、使用期間と使用回数を両方 30 制限する場合は、2つのフラグを両方「1」にする。

【0027】このような構成のデジタル情報管理システムにおいて、デジタル情報販売者は、デジタル情報のダウンロードなどによって利用者にデジタル情報を販売する際や、CD-ROM等の可搬型の記録媒体やプレインス 40 トールによりデジタル情報を既に手に入れている利用者を登録する際に、図示しない入力手段や管理用端末を介して情報管理センタ1の制御手段102に所定の指示を与え、図5に示すフローチャートの手順に従って使用条件格納手段103に格納されている使用条件テーブルの設定を行う。

【0028】まず、使用条件テーブルの登録番号に使われていない番号を1つ選び新しい登録番号Nとする(ステップS11)。次に、販売するデジタル情報本体に登録番号Nを付加する(ステップS12)。これについては後ほど詳しく述べる。次に、使用条件テーブルの新たなエントリに登録番号Nを書き込む(ステップS13)。そして、デジタル情報の内容や利用者との契約により、各種の利用制限の設定を行う。まず、使用期間を制限する場合は(ステップS14→YES)、期間制限フラグを「1」にセットし、許 50

可開始時間と許可終了時間を各々許可開始日時フィールド、許可終了日時フィールドに設定する(ステップS15)。許可開始時間あるいは許可終了時間のどちらか一方を設定する必要がない場合は、そのフィールドを所定の初期値(例えば0)にしておく。使用期間を制限しない場合は(ステップS14→NO)、期間制限フラグを「0」にセットし、許可開始時間と許可終了時間を各々所定の初期値(例えば0)に設定する(ステップS16)。

【0029】使用期間の設定後はステップ17の使用回数の設定に移行する。そして、使用回数を制限する場合は(ステップS17→YES)、回数制限フラグを「1」にセットすると共に、使用可能回数フィールドを設定する(ステップS18)。例えば、3回だけ使用を許可する場合は、このフィールドを「3」とする。使用回数を制限しない場合は(ステップS17→NO)、回数制限フラグを「0」にセットすると共に、使用可能回数フィールドを所定の初期値(例えば0)にする(ステップS19)。以上で使用条件 40 テーブルの設定が終了する。

【0030】さらに、デジタル情報販売者は、図示しない入力手段や管理用端末を介して情報管理センタ1の制御手段102に所定の指示を与え、端末装置2に供給する配布データを作成する。この配布データのフォーマットの例を図6(A)、(B)、(C)、(D)に示す。同図中の登録番号認証子52は情報管理センタ1の認証処理手段104にて作成される。なお、同図に示す配布データは、デジタル情報本体54も一緒に通信回線3または可搬型の記録媒体を介して供給する場合のフォーマットであり、既に、デジタル情報本体54が端末装置2に供給されている場合には、同図に示すフォーマットからデジタル情報本体54を省略した形で作成して端末装置2に供給し、端末装置2内で図6に示すフォーマットに作成し直す。

【0031】図6(A)に示すフォーマットは、基本的なフォーマットであり、ビット長Pのフォーマット種別51、ビット長Qの登録番号認証子52、ビット長Sの登録番号53、ビット長Uの情報本体54が並んだ形式となっている。図6(B)に示すフォーマットは、登録番号53の最後のVビットと情報本体54の最初のVビットが一致しており、共通ビットを重ね合わせて端末装置2のデジタル情報格納手段6に格納するものである。同様に同図(C)に示すフォーマットは、登録番号53の最初のVビットと情報本体54の最後のVビットが一致しており、共通ビットを重ね合わせて端末装置2のデジタル情報格納手段6に格納するものである。同様に同図(D)に示すフォーマットは、登録番号認証子52の最後のVビットと情報本体54の最初のVビットが一致しており、共通ビットを重ね合わせて端末装置2のデジタル情報格納手段6に格納したものである。

【0032】そして、これら図6(B)、(C)、(D)に示すフォーマットとした場合には、端末装置2側で登録番 50

号53や登録番号認証子52を他のデジタル情報の登録番号や登録番号認証子に置き換えると、情報本体の一部のデータも書きかわり、正常に情報本体54を利用することができなくなる。従ってこのような不正行為を抑止することができる。また、重ねあわせた分、デジタル情報格納手段6のメモリ容量を小さくすることができる。なお、図6の(B)、(C)、(D)は一例であり、登録番号あるいは登録番号認証子の一部のビット列と情報本体の一部のビット列を重ね合わせた他のフォーマットを使用しても良い。以下では、このようなフォーマットの代表として同図(B)を例にとって説明する。

【0033】図6に示す配布データにおいて、フォーマット種別51は、登録番号53あるいは登録番号認証子52の一部が情報本体54の一部と重ね合わささせて配置されているか否かを示すフラグである。例えば同図(B)のように重ね合わされている場合に「1」、同図(A)のように重ね合わされていない場合に「0」というように設定されている。また、フォーマット種別51のビット長P、登録番号認証子52のビット長Q、登録番号53のビット長S、および登録番号53と情報本体54の重ね合ったビット長Vは固定長であり、これらの情報は端末装置2の制御手段5に格納管理されている。なお、ビット長Uは情報本体54の内容によって変化する可変長である。

【0034】同図(B)のようなフォーマットを使用する場合には情報管理センタ1において、まず情報本体の先頭からVビットを取り出し、これを登録番号の最後のVビットに割り当てる。そして新たな登録番号がすでに登録されている他の登録番号と同じにならないように、残りの(S-V)ビットを設定する。

$$V_n = F(K_s, N)$$

【0039】

$$V_n = F(K_s, H(N))$$

【0040】以上の処理を行うことにより、図6に示した配布データを作成することができる。次に、利用者が購入したデジタル情報を利用する場合について説明する。利用者が端末装置2の入力手段8を使用して端末装置2の制御手段5に所定の指示を与えると、図8に示すフローチャートに添った処理が行なわれる。

【0041】利用者はまず、端末装置2の入力手段8を使用して利用するデジタル情報を選択する(ステップS21)。この選択情報が供給される制御手段5は選択されたデジタル情報のフォーマット種別51、登録番号認証子52、登録番号53をデジタル情報格納手段6から読み出す(ステップS22)。そして、フォーマット種別51の判別をおこなう(ステップS23)。このフォーマット種別51のデータが「0」の場合には(ステップS23→N0)、登録番号と情報本体の重ね合わせがないフォーマット(図6(A)参照)であるので、そのままステップS25に進む。フォーマット種別51のデータが「1」の場合に

【0035】次に、情報管理センタ1の認証処理手段104の構成を図7に示し、以下に説明する。デジタル情報販売者は、あらかじめ暗号鍵 $K_s$ を作成しておき、この認証処理手段104の暗号鍵格納部81に格納してある。認証処理手段104は、暗号鍵格納部81、暗号関数演算部83、一方向性ハッシュ関数演算部84、及びセクタ85とで構成されており、一方向性ハッシュ関数演算部84は、入力端子から入力される任意の長さの入力データ $X$ から短い固定長のデータ $H(X)$ を演算出力するものである。そして、この演算出力 $H(X)$ から入力データ $X$ を計算するのは極めて困難であり、また複数の異なった $X$ から同一の $H(X)$ の値が得られる確率が極めて小さいことを特徴とする演算部である。

【0036】暗号関数演算部83は、暗号鍵 $K_s$ とある決められた暗号化関数 $F()$ を使って入力データ $Y$ を暗号化する機能を持つ。ここで、暗号鍵 $K_s$ はデジタル情報販売者のみが知り、利用者(端末装置2)には知らせない情報である。したがって、 $F(K_s, Y)$ はデジタル情報販売者(情報管理センタ1)のみが計算することができる。逆に言えば、 $F(K_s, Y)$ が正しく計算されていれば、デジタル情報販売者が計算したということになり、 $F(K_s, Y)$ は認証子としての機能を持つことになる。

【0037】登録番号認証子 $V_n$ は、セクタ85を $f$ 側に設定し、登録番号 $N$ を入力端子に与えて、(1)式の演算による暗号化を行うか、あるいはセクタ85を $e$ 側に設定し、登録番号 $N$ を入力端子に与えて一方向性ハッシュ関数演算部84にて得た値( $H(N)$ )に対して暗号化を行うことにより作成される。この後者の場合は、(2)式の演算を行うことになる。

【0038】

$$\cdots(1)式$$

$$\cdots(2)式$$

は(ステップS23→YES)、登録番号と情報本体の重ね合わせのあるフォーマット(図6(B)参照)であるので、ファイル読み出し位置をVビットだけ戻す(ステップS24)。更に情報本体を読み出す(ステップS25)。そして、登録番号53、登録番号認証子52を情報管理センタ1に送信する(ステップS26)。

【0042】情報管理センタ1の認証処理手段104では、受信した登録番号( $N_r$ )53と登録番号認証子( $V_r$ )52に対して以下のような処理を行い、登録番号53が不正に変更されていないかのチェックを行う(ステップS27)。配布データ作成時に(1)式を使った場合は、セクタ85を $f$ 側に設定して入力端子に受信した登録番号 $N_r$ を与え、暗号関数演算部83によって暗号化関数 $F$ を用いて(3)式の計算を行い、出力 $V_o$ を得る。また配布データ作成時に(2)式を使った場合は、セクタ85を $e$ 側に設定して入力端子に受信した登録番号 $N_r$ を与え、暗号関数演算部83によって暗号化関数 $F$ を用いて(4)式の計

算を行い、出力Voを得る。

$$Vo = F(Ks, Nr)$$

【0044】

$$Vo = F(Ks, H(Nr))$$

【0045】そして、登録番号認証子Vrと出力Voが一致するかチェックする。Vr≠Voであれば(ステップS27→N0)、登録番号53が不正に変更されていることになるので、使用禁止を意味するデータを端末装置2に送信する(ステップS28)。また、Vr=Voであれば(ステップS27→YES)、登録番号53は不正に変更されていないと判定できるので、ステップS29に進む。ステップS29では、登録番号Nrが使用条件テーブルに登録されているかのチェックを行う。もし登録されていなければ(ステップS29→N0)、その登録番号Nrは偽造されたものであると見なし、使用禁止を意味するデータを端末装置2に送信する(ステップS28)。

【0046】そして、登録番号Nrが使用条件テーブルに登録されている場合は(ステップS29→YES)、さらに、期間制限フラグが「1」にセットされているか否かをチェックする(ステップS30)。期間制限フラグが「0」の場合は(ステップS30→N0)、特に期間制限が設定されていないので、そのままステップS32へ進む。期間制限フラグが「1」にセットされている場合には(ステップS30→YES)、現在日時が許可開始日時と許可終了日時との間にあることを確認する(ステップS31)。そして、現在日時が許可開始日時と許可終了日時との間にある場合には(ステップS31→YES)、ステップS32へ進む。

【0047】このステップS31において、(期間制限フラグが「1」であり、)許可開始日時あるいは許可終了日時が所定の初期値である場合は、初期値である項目に関し許可条件を満たすと見なす。すなわち、許可開始日時が初期値であれば、許可終了日時のみチェックし、現在日時が許可終了日時以前であればステップS32へ進む。同様に、許可終了日時が初期値であれば、許可開始日時のみチェックし、現在日時が許可開始日時以降であればステップS32へ進む。また、許可期間内でなければ(ステップS31→N0)、ステップS28に進み、使用禁止を意味するデータを端末装置2に送信する。

【0048】ステップS32では回数制限フラグが「1」にセットされているかチェックする。回数制限フラグが「0」の場合は(ステップS32→N0)、特に使用回数の制限がないのでそのままステップS35に進む。回数制限フラグが「1」にセットされている場合は(ステップS32→YES)、使用可能回数が「0」より大きいかをチェックする(ステップS33)。そして、使用可能回数が「0」の場合は(ステップS33→N0)、ステップS28に進み、使用禁止を意味するデータを端末装置2に送信する。使用可能回数が「0」でない場合には、その使用可能回数を1だけ減じ(ステップS34)、ステップS35へ進む。そして、以上の判定により、正当な使用であると確認された場合には使

【0043】

…(3)式

…(4)式

用許可を意味するデータを端末装置2に送信する(ステップS35)。

【0049】端末装置2の制御手段5は、通信回線3及び通信手段4を介して情報管理センタ1から受け取ったデータが使用許可であるか否かをチェックして(ステップS36)、使用許可であれば(ステップS36→YES)、デジタル情報本体をデジタル情報格納手段6から読みだしてデジタル情報のフォーマットに従った処理を行い、ディスプレイ、スピーカ等の出力手段9に出力する(ステップS37)。また、情報管理センタ1から受け取ったデータが使用禁止であれば、その旨のエラーメッセージを出力手段9に出力し処理を終了する(ステップS38)。このように処理を行うことにより、正規に登録し、使用期間、回数制限を守っている正当な端末装置(利用者)にだけ、デジタル情報の使用許可を与えることができる。

【0050】

【発明の効果】本発明のデジタル情報管理システム及びデジタル情報管理方法は、単にデジタル情報の不正コピーを防止するだけでなく、使用期間、使用回数、あるいはその両方を限定してデジタル情報を利用させることが可能となる。厳密には、デジタル情報のコピー行為そのものは可能であるが、使用回数を制限した場合には、デジタル情報を正当な方法で入手した利用者が別の利用者にデジタル情報のコピーを渡しても、コピーを入手した別の利用者が使用した回数だけ元の利用者の使用できる回数が減ってしまうので、元の利用者が不利益を被るので、このような行為(デジタル情報のコピー)を十分抑制できる。

【0051】また、正当な利用者が、例えば自宅と仕事場の2個所でデジタル情報を使用したい場合には、別々の端末装置にデジタル情報をコピーして、それぞれの端末装置で、正当に利用することができる。この場合でも、使用回数が制限されている場合には、それぞれの端末装置で使用された回数の合計で使用回数の制限が行われるので、情報提供者が被害を受けることはない。さらに、デジタル情報の使用条件や使用状況を全て情報管理センタで記録管理するので、端末装置の利用者がこれらの情報を不正に変更することは非常に困難となる。

【0052】一方、利用者にとっては、個別のニーズに応じて使用期間や使用回数を細かく設定した購入ができるので、これらの条件を設定しない売り切りの場合よりも無駄がなく、実質的に安い料金で必要な情報を必要にだけ利用することができる。また、デジタル情報を端末装置に格納して使用許可情報だけを端末装置に送信する方式なので、端末装置にデジタル情報を蓄積せず利用の度にセンタからダウンロードする従来の方式と比べて、



通信コストが安く済み、利用する際の待ち時間も少なくなるという優れた効果がある。

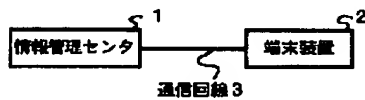
【0053】また本発明では、デジタル情報本体に固有の登録番号と登録番号認証子が情報管理センタにより付与されており、情報センタだけが知る暗号鍵がないと登録番号認証子は作成できないので、利用者が登録番号を偽造して不正にデジタル情報を使うことは非常に困難である。

【0054】さらに本発明は、端末装置内に暗号処理機能を必要とせず、端末装置内に暗号鍵を格納していない。すなわち端末装置に複雑な処理機能や機密性を要求される部分がない。従って端末装置に特殊な装置を付加することなく、一般的な構成のコンピュータを端末装置として構成することができるので、端末装置のコストが従来より安くなると同時に、より多くのユーザが利用可能となる。また、一般的な構成のコンピュータを端末装置として構成することができることにより、デジタル情報を利用する端末装置の種類が限定されないので、利用者はデジタル情報を複数の異なった端末装置からでも利用することができ、利用者の利便性が向上するという効果がある。

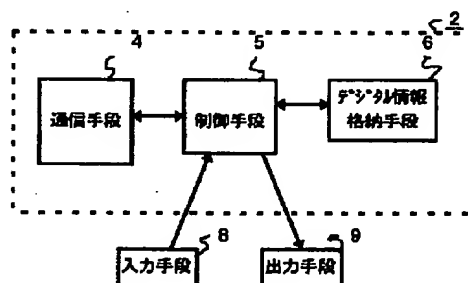
【0055】さらに、登録番号あるいは登録番号認証子の一部のビット列と情報本体の一部のビット列を一致させ、その一致部分を端末装置内で重ね合わせて格納することにより、端末装置で行われる不正な改変にも対応することができる。

【図面の簡単な説明】

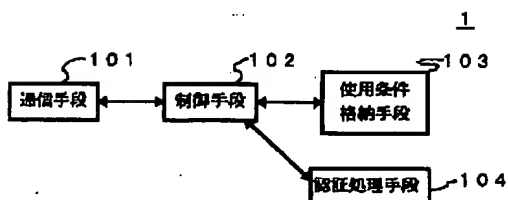
【図1】



【図2】



【図3】



【図4】

登録番号	期限制御フラグ	回数制御フラグ	許可開始日時	許可終了日時	使用回數
N	0	1	0	0	3

【図1】本発明のデジタル情報管理システムの一実施例を示す構成図である。

【図2】本発明のデジタル情報管理システムの端末装置例を示す構成図である。

【図3】情報管理センタを示す構成図である。

【図4】使用条件テーブルを説明するための図である。

【図5】使用条件テーブルの設定方法を説明するフローチャート図である。

【図6】端末装置に供給するデータフォーマットの例を示す構成図である。

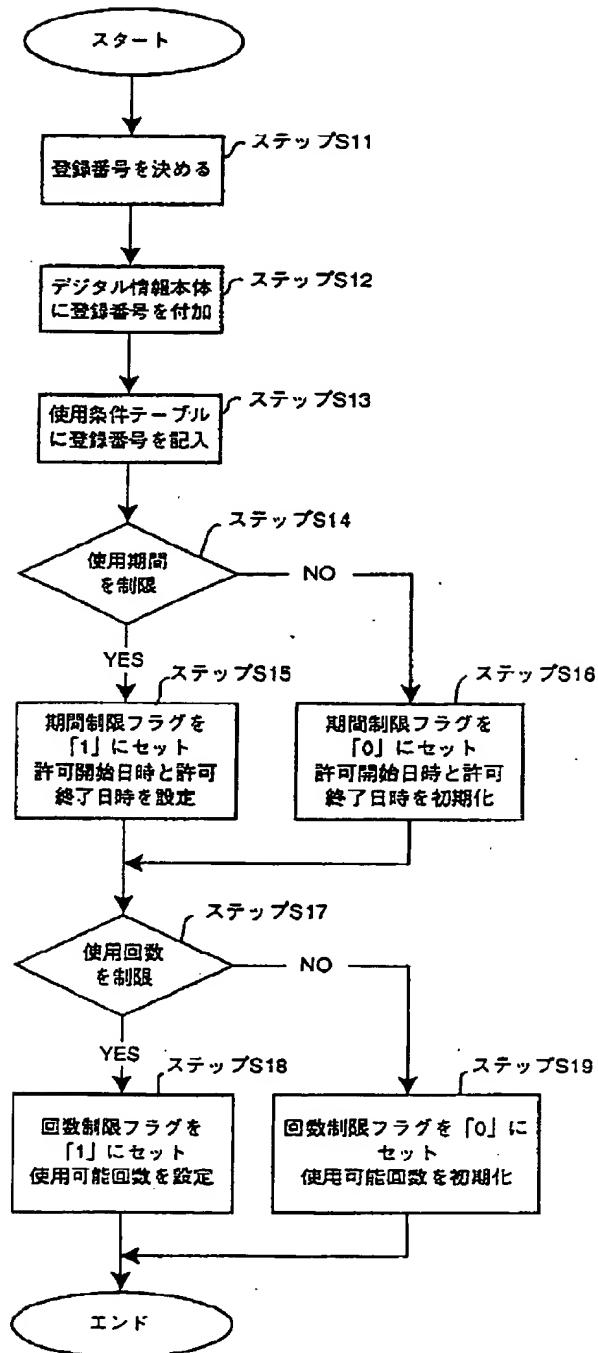
【図7】本発明の情報処理センタの認証処理手段の例を示す構成図である。

【図8】デジタル情報の利用手順を説明するためのフローチャート図である。

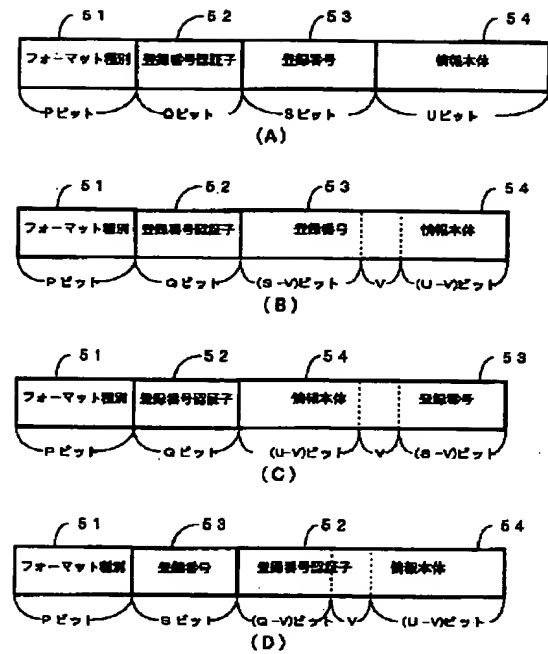
【符号の説明】

- 1 情報管理センタ
- 2 端末装置
- 3 通信回線
- 4 通信手段 (第1の通信手段)
- 5 制御手段 (第1の制御手段)
- 6 デジタル情報格納手段
- 8 入力手段
- 9 出力手段
- 101 通信手段 (第2の通信手段)
- 102 制御手段 (第2の制御手段)
- 103 使用条件格納手段
- 104 認証処理手段

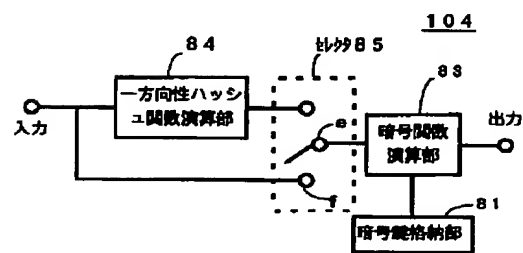
【図5】



【図6】



【図7】



【図8】

